EXHIBIT 49

This article was published more than **2 years ago**

The Washington Post
Democracy Dies in Darkness

YOUR DATA AND PRIVACY

How to block Facebook from snooping on you

Seven steps you can take to keep Facebook and Instagram from gathering so much of your personal information outside of their apps

Perspective by Geoffrey A. Fowler
Columnist | + Follow

Updated September 29, 2021 at 9:54 a.m. EDT | Published August 29, 2021 at 8:00 a.m. EDT

If you ever get that eerie feeling Facebook or Instagram is listening to you, you're not entirely hallucinating.

Facebook says it's not literally activating the microphones on our smartphones, but it is tracking what we do in other apps, websites and even real-world stores. That much data can make ads feel as on-point as if it were in the room. In a recent column, I investigated everything Facebook can passively learn about you, even when you stop using it for long stretches.

Don't be fooled by the kinder, gentler image of Instagram, either: It's owned by Facebook and does the same kind of tracking as Facebook.

So what can you do about it? If you're very committed — or a bit techie — there are some steps you can take to try to hide from Facebook's personal data vacuum.

I polled some of the smartest privacy experts about evasive maneuvers they recommend, including the Electronic Frontier Foundation's Bennett Cyphers, Disconnect's Patrick Jackson, former chief technologist for the Federal Trade Commission Ashkan Soltani and Jumbo Privacy's Pierre Valade. Stopping the snooping entirely would be really difficult, so I focused this advice on steps that could make the biggest impact.

Just remember: These changes only affect what Facebook and Instagram can learn about you *outside* of their apps. Everything you and your friends do inside the apps — from tapping the "Like" button to posting status updates and profile information — will still feed the company personal information. (And anything you make public can be seen by people and companies alike.)

Here are seven steps to stop Facebook tracking, starting with the nuclear option.

1. Quit Facebook and Instagram

They'll beg you to stay, and encourage you to just temporarily "deactivate" your account for a while. But if you do fully delete your accounts on both services, Facebook will no longer build out a profile with your activities to target ads.

To completely delete your Facebook account:

- Click on this link in a browser where you're logged in to Facebook.
- Select Permanently Delete Account, then click on Continue to Account Deletion.
- Click Delete Account, enter your password and continue and say goodbye forever.

Before you do this, you might want to download a copy of the data from your Facebook account. Use this link.

To quit Instagram, it's a similar process:

- Click on this link in a web browser where you're logged in to Instagram.
- Pick a reason, such as privacy concerns.
- Tap Delete.

There is one privacy downside to quitting Facebook: The company still receives and collects data about people who don't have accounts. The only way you can actually see what it knows about you is to maintain an account.

2. Change these Facebook privacy settings

Facebook has lots of bad default settings you should change. But the most important one to combat tracking is called Off-Facebook Activity. (Read a column I wrote about it here.)

Your Off-Facebook Activity settings are easiest to access on the Web by clicking this link.

- You'll see a page that shows you the apps, websites and other businesses where Facebook has been tracking you.
- Tap More Options, then Manage Future Activity, then toggle Future Off-Facebook Activity to off.

While you're at it, I also recommend changing a setting that gives Facebook permission to connect into other apps and websites. Just know that adjusting this setting would keep you from logging into apps where you used Facebook to set up your account.

- Access your apps and websites setting page with this link.
- Tap Turn Off next to apps, websites and games.

3. Limit app tracking on your phone

Starting in the spring of 2021, Apple began letting iPhone owners tell apps like Facebook and its many partners to do less tracking. (Read more about how it works here.)

Each app can ask your permission individually, but it's most efficient to go in and change one universal setting for your iPhone:

- Go to Settings, then Privacy, then Tracking.
- Make sure Allow Apps to Request to Track is switched to off. The virtual button should be on the left, not showing any green, to indicate this.

Google has announced a version of this is coming to Android phones starting at some point in 2021. In the phone privacy settings, look for an option that lets you opt out of ad personalization. (By early 2022, you should be able use this setting on any Android app that came from the Google Play store, regardless of the version of Android you're running.)

Note: You'll need to adjust this setting on every one of your devices, including tablets like iPads.

4. Bolster your Web browser

When it comes to your privacy, not all Web browsers are built the same. The most popular one, Google's Chrome, does nothing to stop Facebook, along with a lot of other companies, from tracking how you surf the Web. (Read more about how Chrome enables tracking here.)

The Firefox browser, made by the nonprofit Mozilla, combats some forms of website tracking by default. So do Brave, Apple's Safari and Microsoft's latest Edge.

To take your protection a step further, Mozilla makes a special extension called the Facebook Container. It puts Facebook in a special virtual tab where it can't interact with other websites at all.

If you want to stick with Chrome, consider adding a privacy extension such as Privacy Badger or DuckDuckGo that also helps block Facebook trackers, as well as ones from lots of other companies, too.

5. Block more app trackers

Like those extensions do for Web browsers, iPhone services such as Lockdown Privacy or Disconnect's Privacy Pro block even more trackers hidden inside apps — including ones that might be working for Facebook.

Unfortunately, Google hasn't let tracker-blockers like these in its Play Store for Android phones.

A related idea: Use the Facebook website on your iPhone, instead of the app. The mobile Safari browser won't let it as easily use cookies and tracker pixels or grab personal data such as your location and won't continue sipping data in the background when you're not using the browser.

6. Obscure your email

One way Facebook learns about you is when other companies send it your email address (or phone number or some other way to identify you). Facebook then matches up this info with the account associated with that email.

So give Facebook a throwaway, burner email — one you never really check or hand out to other companies. That might make it harder for Facebook to find you.

If you have an iPhone, the Sign In With Apple service included with the iOS operating system creates a different throwaway email address for every single app you use it with. That's an even better way to make sure companies can't cross reference who you are.

I haven't tested it myself recently, but you could also subscribe to a service such as Abine's Blur, which lets you create not only burner emails but also credit card numbers.

7. Tell companies to stop selling your data

Laws such as the California Consumer Privacy Act give us the right to tell companies to stop sharing, or "selling," our data to Facebook and others.

The only problem: You have to tell them to knock it off one by one.

This can be a lot of work. But if you've got some time, you might want to start with data brokers, who are in the business of collecting your personal information from all over and then reselling it. California keeps a useful list of data brokers on the state attorney general's website.

Got other tactical steps to stop Facebook snooping — or questions about how to make this work for you? I'd love to hear them on email or through our Washington Post Help Desk.